Joint Learning of Assignment and Representation for Biometric Group Membership

Marzieh Gheisari, Teddy Furon, Laurent Amsaleg

▶ **To cite this version:**

Marzieh Gheisari, Teddy Furon, Laurent Amsaleg. Joint Learning of Assignment and Representation for Biometric Group Membership. ICASSP 2020 - 45th International Conference on Acoustics, Speech, and Signal Processing, May 2020, Barcelona, Spain. hal-02490005

HAL Id: hal-02490005
https://hal.science/hal-02490005

Submitted on 26 Feb 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

JOINT LEARNING OF ASSIGNMENT AND REPRESENTATION FOR BIOMETRIC GROUP MEMBERSHIP

Marzieh Gheisari, Teddy Furon, Laurent Amsaleg,

Univ Rennes, Inria, CNRS, IRISA, France

{ marzieh.gheisari-khorasgani, teddy.furon}@inria.fr, laurent.amsaleg@irisa.fr

ABSTRACT

This paper proposes a framework for group membership protocols preventing the curious but honest server from reconstructing the enrolled biometric signatures and inferring the identity of querying clients. This framework learns the embedding parameters, group representations and assignments simultaneously. Experiments show the trade-off between security/privacy and verification/identification performances.

***Index Terms*—** Group Representation, Verification, Identification, Security, Data Privacy.

1. INTRODUCTION

Group membership verification is a procedure checking whether an item or an individual is a member of a group. If membership is positively established, then an access to some resources (buildings, wifi, payment, conveyor units, ...) is granted; otherwise the access is refused. Being granted with this shared privileged access requires that the members of the group could be distinguished from non-members, but it does not require to distinguish members from one another. Indeed, privacy concerns suggest that the verification should be carried-out anonymously.

This paper studies group verification and also group identification. In this later setup, there are several groups of members and one needs to identify in which group the user is belonging to. This paper focuses on privacy preserving group identification procedure where group identity of a member is found without disclosing the identity of that individual.

In computer vision, it is very common to aggregate signals into one representation [1, 2, 3], but they do not consider security or privacy. For instance, in [4], Iscen *et al.* use the *group testing* paradigm to pack a random set of image signatures into a unique high-dimensional vector where the similarities between the original non-aggregated signatures and a query signature is preserved through the aggregation.

Recently [5, 6, 7] proposed a framework based on aggregation and embedding of several biometric signatures into a unique vector representing the members of a group. It has been demonstrated that this allows a good assessment of the membership property at test time provided that the groups are small. It has also been shown that this provides privacy and security. Privacy is enforced because it is impossible to infer from the aggregated feature which original signature matches the one used to probe the system. Security is preserved since nothing meaningful leaks from embedded data [8, 9].

This paper revisits the core mechanism proposed by [6]. That work, however, is deterministic in the sense that it learns group representations based on predefined groups. This paper shows that learning jointly the group representations and group assignments results in better performance without damaging the security. This adresses scenarios where the number of members is too big. Their signatures can not be packed into one unique group representation with a technique like [6]. Therefore, members are automatically assigned to different groups. A light cryptographic protocol is deployed to secure their privacy during group verification.

2. GROUP MEMBERSHIP

2.1. Notations

The embedding, the assignment, and the group representations are learned jointly at enrolment, and given to a server. Biometric signatures are modelled as vectors in $\mathbb{R}^d$. $\mathbf{X} \in \mathbb{R}^{d \times N}$ is the matrix of the signatures to be enrolled into M groups. The group representations are stored column wise in $\ell \times M$ matrix $\mathbf{R}$. The group representations are quantized and sparse *i.e.*, $\mathbf{r}_g \in \mathcal{A}^\ell$ with $\mathcal{A} = \{-1, 0, +1\}$ and $\|\mathbf{r}_g\|_0 \leq S < \ell, \forall g \in [M]$.

At query time, the user computes a sparse representation of his biometric signature $\mathbf{q} \in \mathbb{R}^d$. For that purpose, function $\mathsf{e} : \mathbb{R}^d \to \mathcal{A}^\ell$ maps a vector to a sequence of ℓ discrete symbols. We use the sparsifying transform coding [8, 9]: $\mathbf{p} := \mathsf{e}(\mathbf{q}) = \mathsf{T}_S(\mathbf{W}^\top \mathbf{q})$. After projecting $\mathbf{q} \in \mathbb{R}^d$ on the column vectors of $\mathbf{W} \in \mathbb{R}^{d \times \ell}$, the output alphabet $\mathcal{A}$ is imposed by the ternarization function T_S: The $\ell - S$ components having the lowest amplitude are set to 0. The S remaining ones are quantized to +1 or -1 according to their sign.

2.2. Formulation of the optimization problem

Our group membership protocol aims at jointly learning the partition, the embedding and the group representations. The key is to introduce the auxiliary data $\mathbf{E} = [\mathbf{e}_1, \ldots, \mathbf{e}_N] \in \mathcal{A}^{\ell \times N}$ the hash codes of enrolled signatures and $\mathbf{Y} \in \mathbb{R}^{M \times N}$ the group indicator matrix ($y_{i,j} = 1$ if $\mathbf{e}_j$ is assigned to i-th group). Then, the optimization problem is composed of a cost

Research supported by the ERA-Net project ID_IoT 20CH21_167534.

for embedding C^E and a cost for partitioning $C^{A,G}$:

$$\min_{\mathbf{W},\mathbf{R},\mathbf{Y}} C^E(\mathbf{X},\mathbf{W},\mathbf{E}) + C^{A,G}(\mathbf{E},\mathbf{Y},\mathbf{R}), \tag{1}$$

The embedding cost is the loss for quantizing signatures:

$$C^E(\mathbf{X},\mathbf{W},\mathbf{E}) \quad := \quad \sum_{i=1}^{N} \left\|\mathbf{e}_i - \mathbf{W}^\top \mathbf{x}_i\right\|_2^2. \tag{2}$$

The assignment aims at grouping together signatures sharing similar hash codes: the overall dissimilarity between members and their group representation is minimized while the separation between two groups is maximized. Inspired by Linear Discriminant Analysis, we consider variance to measure dissimilarity. The within group scatter matrix $\mathbf{S}_w$ and the between group scatter matrix $\mathbf{S}_b$ are defined as

$$\begin{aligned}
\mathbf{S}_w &= \sum_{g=1}^{M} \sum_{i \in \mathcal{Y}_g} (\mathbf{e}_i - \mathbf{r}_g)(\mathbf{e}_i - \mathbf{r}_g)^\top = (\mathbf{E} - \mathbf{RY})(\mathbf{E} - \mathbf{RY})^\top \\
\mathbf{S}_b &= \sum_{g=1}^{M} \mathbf{r}_g \mathbf{r}_g^\top = \mathbf{RY}(\mathbf{RY})^\top
\end{aligned}$$

where $\mathcal{Y}_g = \{i \in [N] : y_{g,i} = 1\}$. The cost for partitioning is $C^{A,G} = \lambda Tr(\mathbf{S}_w) - \gamma Tr(\mathbf{S}_b)$ for some λ, γ in $\mathbb{R}_+$.

In the end, the objective function is formulated as:

$$\begin{aligned}
\min_{\mathbf{W},\mathbf{R},\mathbf{Y}} \quad & \|\mathbf{E} - \mathbf{W}^\top \mathbf{X}\|_F^2 + \lambda Tr(\mathbf{S}_w) - \gamma Tr(\mathbf{S}_b) \\
\text{s.t.} \quad & \mathbf{W}^T\mathbf{W} = \mathbf{I}_\ell \\
& \mathbf{Y} \in \{0,1\}^{M \times N}, \ \ \|\mathbf{y}_i\|_1 = 1 \ \forall i \in [N] \\
& \mathbf{e}_i \in \mathcal{A}^\ell, \ \ \|\mathbf{e}_i\|_0 \leq S \\
& \mathbf{r}_g \in \mathcal{A}^\ell, \ \ \|\mathbf{r}_g\|_0 \leq S
\end{aligned} \tag{3}$$

The constraint on $\mathbf{Y}$ ensures that each signature belongs to exactly one group.

2.3. Suboptimal solution

The solution of (3) is found by iterating the following steps:

W-Step. We fix $\mathbf{E}$, $\mathbf{R}$, $\mathbf{Y}$ and update $\mathbf{W}$ by solving:

$$\begin{aligned}
\min_{\mathbf{W}} \quad & \left\|\mathbf{E} - \mathbf{W}^\top \mathbf{X}\right\|_F^2 \\
\text{s.t.} \quad & \mathbf{W}^\top \mathbf{W} = \mathbf{I}_\ell
\end{aligned} \tag{4}$$

This problem is a least square Procruste problem with orthogonality constraint. By setting $\mathbf{S} := \mathbf{X}\mathbf{E}^\top$, [10] shows that $\mathbf{W} = \mathbf{U}\mathbf{V}^\top$, where $\mathbf{U}$ contains the eigenvectors corresponding to the ℓ ($\ell < d$) largest eigenvalues of $\mathbf{S}\mathbf{S}^\top$ and $\mathbf{V}$ contains the eigenvectors of $\mathbf{S}^\top\mathbf{S}$.

E-Step. Given $\mathbf{W}$, $\mathbf{Y}$ and $\mathbf{R}$, (3) amounts to:

$$\begin{aligned}
\min_{\mathbf{E}} \quad & \left\|\mathbf{E} - \mathbf{W}^\top \mathbf{X}\right\|_F^2 + \lambda \left\|\mathbf{E} - \mathbf{RY}\right\|_F^2 \\
\text{s.t.} \quad & \mathbf{e}_i \in \mathcal{A}^\ell, \ \ \|\mathbf{e}_i\|_0 \leq S
\end{aligned} \tag{5}$$

We first find the solution relaxing the constraints and then apply ternarization function T_S to obtain sparse codes:

$$\mathbf{E} = \mathsf{T}_S(\mathbf{W}^\top \mathbf{X} + \lambda \mathbf{RY}). \tag{6}$$

(R,Y)-Step. When fixing $\mathbf{W}$ and $\mathbf{E}$, the assignment and group representations are found by minimizing:

$$\begin{aligned}
\min_{\mathbf{R},\mathbf{Y}} \quad & \|\mathbf{E} - \mathbf{RY}\|_F^2 - \frac{\lambda}{\gamma} Tr(\mathbf{RYY}^\top \mathbf{R}^\top) \\
\text{s.t.} \quad & \mathbf{Y} \in \{0,1\}^{M \times N}, \ \ \|\mathbf{y}_i\|_1 = 1 \ \forall i \in [N] \\
& \mathbf{r}_g \in \mathcal{A}^\ell, \ \ \|\mathbf{r}_g\|_0 \leq S
\end{aligned} \tag{7}$$

As $\mathbf{E}$ is fixed, $Tr(\mathbf{E}\mathbf{E}^\top)$ is irrelevant to $\mathbf{Y}$, thus minimizing (7) is equivalent to:

$$\min_{\mathbf{R},\mathbf{Y}} \quad \left\| \frac{\lambda}{\lambda - \gamma} \mathbf{E} - \mathbf{RY} \right\|_F^2. \tag{8}$$

Relaxing the ternarization constraint, (8) is solved by a k-means clustering algorithm, *i.e.*iteratively:

- *Update assignments*: Each item is assigned to its nearest group representative.
- *Update centroids*: g-th centroid is the mean of all $\tilde{\mathbf{e}}_i$ in group g.

Then the group representation $\mathbf{r}_g$ is found by applying ternarization function on g-th centroid.

3. EXPERIMENTS

This section presents the datasets used in our experiments and investigates the performance of the proposed method for two application scenarios. We compare our scheme with EoA-SP, AoE-SP [5] and EoA-ML, AoE-ML [6]. For the baselines N individuals of each dataset are enrolled into M random groups but for our scheme the algorithm learns how to partition the enrolled templates.

3.1. Datasets

3.1.1. Face Datasets

Face descriptors are obtained from a pre-trained network based on VGG-Face architecture [11] followed by PCA and then L_2-normalization with $d = 1,024$.

LFW [12]. These are pictures of celebrities in all sort of viewpoint and under an uncontrolled environment. We use pre-aligned LFW images. The enrollment set consists of $N = 1680$ individuals with at least two images in the LFW database. One random template of each individual is enrolled in the system, playing the role of $\mathbf{x}_i$. Some other $N_q = 263$ individuals were randomly picked in the database to play the role of impostors.

CFP [13]. These are frontal and profile views of celebrities taken in an uncontrolled environnement. We use $N = 400$ frontal images to be enrolled in the system. The impostor set is a random selection of $N_q = 100$ other individuals.

3.1.2. IRIS Datasets

Iris images are prepossessed by the following steps: iris localization, iris normalization and image enhancement. Then

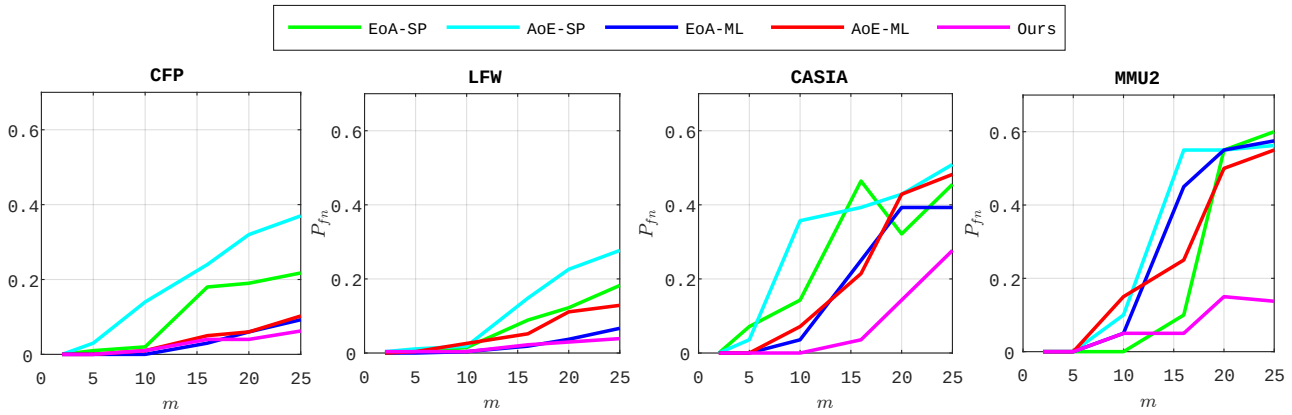

Fig. 1: Performances comparison for varying group size m. P_{fn} at $P_{\mathsf{fp}} = 0.05$ for group verification.

the feature vectors are extracted by Gabor filters.

CASIA-IrisV1 [14]. The database includes 756 iris images from 108 eyes of Chinese persons. The images stored in the database were captured within a highly constrained capturing environment. 3 images were collected in a first session and 4 images in a second session. The database is created by randomly sampling $N = 80$ individuals to be enrolled, and $N_q = 28$ impostors.

MMU2 [15]. This dataset contains 995 images corresponding to 100 people with different age and nationality from Asia, Middle East, Africa and Europe. Each of them contributes to 5 iris images for each eye. We exclude 5 left eye iris images due to cataract disease.

3.2. Group Verification

A user claims she/he belongs to group g. This claim is true under hypothesis $\mathcal{H}_1$ and false under hypothesis $\mathcal{H}_0$ (*i.e.* the user is an impostor). Her/his signature $\mathbf{q}$ is embedded into $\mathbf{p} = \mathsf{e}(\mathbf{q})$, and $(\mathbf{p}, g)$ is sent to the system, which compares $\mathbf{p}$ to the group representation $\mathbf{r}_g$. The system accepts $(t = 1)$ or rejects $(t = 0)$ the claim. This is a two hypothesis test with two probabilities of errors: $P_{\mathsf{fp}} := \mathbb{P}(t = 1|\mathcal{H}_0)$ is the false positive rate and $P_{\mathsf{fn}} := \mathbb{P}(t = 0|\mathcal{H}_1)$ is the false negative rate. The figure of merit is P_{fn} when $P_{\mathsf{fp}} = 0.05$.

Fig. 1 compares the performance of our scheme with baselines for group membership verification. Totally our scheme gives a better verification performance especially on CASIA. Since our method tries to simultaneously learn group representations and assignment, it aggregates similar embedded vectors and this looses less information.

Note that, although LFW and CFP are difficult datasets due to the "in the wild" variations, the group membership verification task is handled well even for large group sizes. This is not the case for iris datasets. As mentioned before, we make use of VGG-Face for face datasets while for iris, traditional feature extraction algorithms are used. So, the big difference in overall analysis shows how the feature space affect the performance of group membership tasks.

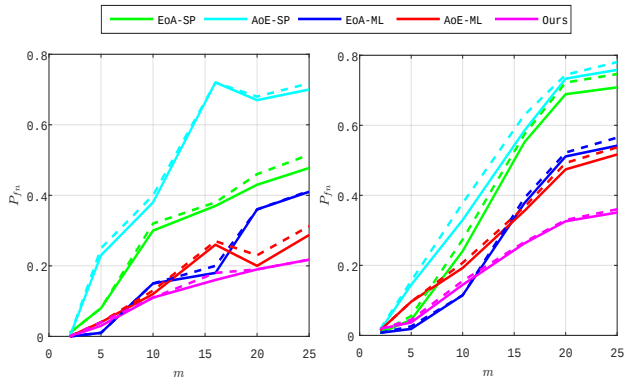

Fig. 2: Performances comparison for varying group size m on group identification for CFP(left) and LFW(right). P_{fn} at $P_{\mathsf{fp}} = 0.05$ for the first step of group identification (solid) and P_ϵ for the second step of group identification (dashed).

3.3. Group Identification

The scenario is an open set identification where the querying user is either enrolled or an impostor. The system proceeds in two steps. First, it decides whether or not this user is enrolled. This is verification as above, except that the group is unknow: The system computes $\delta_j = \|\mathbf{p} - \mathbf{r}_j\|, \forall j \in [M]$, and accepts $(t = 1)$ if the minimum of these M distances is below a given threshold τ. The figure of merit is P_{fn} when $P_{\mathsf{fp}} = 0.05$.

When $t = 1$, the system proceeds to the second step. The estimated group is given by $\hat{g} = \arg\min_{j\in[M]} \delta_j$. The figure of merit for this second step is $P_\epsilon := \mathbb{P}(\hat{g} \neq g)$ or the Detection and Identification Rate $DIR := (1 - P_\epsilon)(1 - P_{\mathsf{fn}})$.

Fig. 2 shows that our scheme brings improvement compared to the baselines and the improvement is also better as the size of groups increases.

The impact of the group size on DIR is illustrated in Fig. 3. Obviously, packing more signatures into one group representation is detrimental. It gets worse when the queries are not well correlated with the enrolled signature.

3.4. Security and Privacy Analysis

A curious server can only reconstruct a single vector $\hat{\mathbf{r}}_g = \mathsf{rec}(\mathbf{r}_g)$ from the group representation $\mathbf{r}_g$, and this vector

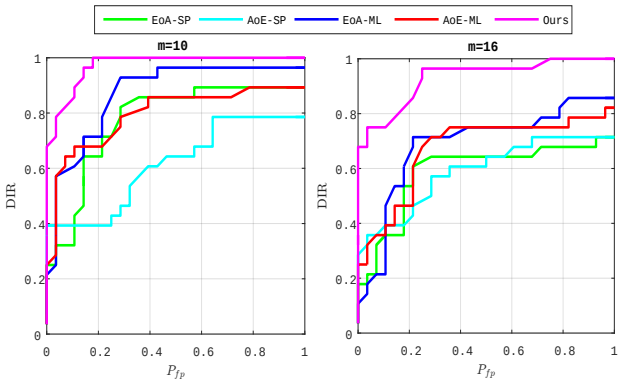

Fig. 3: The Detection and Identification Rate (DIR) vs. P_{fp} for group identification on CASIA-IRISV1.

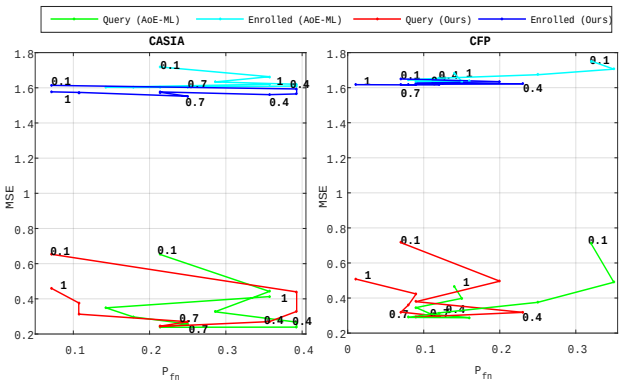

Fig. 4: Investigation of trade-off between security and performance for varying sparsity level S on CFP (with $m = 25$) and CASIA-IrisV1 (with $m = 16$).

serves as an estimation of any signature in the group. We measure the security by the mean square error over the dataset:

$$\mathsf{MSE}_S = (dN)^{-1} \sum_{g=1}^{M} \sum_{i=1}^{|\mathcal{Y}_g|} \mathbb{E}(\|\mathbf{x}_i - \hat{\mathbf{r}}_g\|^2). \tag{9}$$

For the of privacy of query template, a curious server can reconstruct the query template $\mathbf{q}$ from its embedding:

$$\mathsf{MSE}_P = d^{-1}\mathbb{E}(\|\mathbf{Q} - \mathsf{rec}(\mathsf{e}(\mathbf{Q}))\|^2), \tag{10}$$

These reconstructions are possible only if matrix $\mathbf{W}$ is known. This is not the case in practice, so we give here an extra advantage to the curious server. Figure 4 compares security with AoE-ML [6] where the assignment was imposed randomly, *i.e.* not learned. Different levels of sparsity are tested. The reconstruction error of queries are close in either case, yet learning the assignment improves verification performance. Reconstructing enrolled signatures is more difficult due to the aggregation. However, learning the assignment by similarity correspondence in the embedded domain decreases the security slightly while improving the performance a lot.

4. SECURITY PROTOCOLS

This section gives an example of a cryptographic protocol exploiting the group representations. The experimental section showed that grouping secures the enrolled signatures, but ternarization alone provides less protection to the query. Therefore, this protocol strengthens the protection of the querying user. For security reason, the server only manipulates query and the distances in the encrypted domain. For privacy reason, the server only learns that the query is close enough to one group representation, but it cannot tell which group exactly. We assume honest but curious user and server.

This protocol also justifies choices of our scheme: Queries and group representations are heavily quantized onto a small alphabet $\mathcal{A}$. They are long vectors but sparse: only S components will be processed in the encrypted domain. Moreover, we have $\|\mathbf{p} - \mathbf{r}\|^2 \in [0, 2S]$. These facts ease the use of partial homomorphic encryptions with limited module, whence a low complexity and expansion factor. The group representations remain in the clear on the server side, and we do not need fully homomorphic encryption.

The user generates a pair of secret and public keys (sk_U, pk_U) for an additive homomorphic cryptosystem $e(\cdot)$ (say [16]), and sends the query encrypted component-wise. The server computes its correlation with group representation $\mathbf{r}_g$:

$$e(\mathbf{p}^\top \mathbf{r}_g, pk_U) = \prod_{i:r_g(i)\neq 0} e(p(i), pk_U)^{r_g(i)}. \tag{11}$$

The server also generates a key pair (sk_S, pk_S) for a multiplicative homomorphic cryptosystem $E(\cdot)$ (say [17]), and sends the user $(E(e(\mathbf{p}^\top \mathbf{r}_g, pk_U), pk_S))_g$. The user randomly permutes the order of these quantities and masks them by multiplying them by $E(1, pk_S)$. This yields another semantically secure version of the ciphertexts thanks to the multiplicative homomorphy of $E(\cdot)$. The server decrypts $(e(\mathbf{p}^\top \mathbf{r}_k, pk_U))_k$, but the permutation prevents connecting k back to the group index g. Again thanks to homomorphy, the server computes $(e(a_k(2S - 2\mathbf{p}^\top \mathbf{r}_k - \tau) + b_k), pk_U))_g$ where (a_k, b_k) are random signed integers. The user decrypts and sends $(a_k(\|\mathbf{p} - \mathbf{r}_k\|^2 - \tau) + b_k)_k$ to the server. The user cannot guess the distances $\|\mathbf{p} - \mathbf{r}_k\|^2$ thanks to the masking $(a_k, b_k)_k$, not even the sign of $(\|\mathbf{p} - \mathbf{r}_k\|^2 - \tau)$. The server can do this (since it knows (a_k, b_k)) and thus learns whether there is one group where $(\|\mathbf{p} - \mathbf{r}_k\|^2 - \tau)$ is negative.

5. CONCLUSION

We proposed a method for group membership verification and identification jointly learning group representations and assignment. The idea is to minimize the overall distance between group members while maximizing the separation between groups in the embedded domain. Yet, the method still has some rigidness: the prototyping of the embedding (the sparse ternary quantization), considering mean as group centroids, and assigning a signature to only one group.

6. REFERENCES

[1] J. Sivic and A. Zisserman, "Video google: a text retrieval approach to object matching in videos," in *Proceedings of the IEEE International Conference on Computer Vision*, 2003.

[2] Hervé Jégou, Florent Perronnin, Matthijs Douze, Jorge Sánchez, Patrick Pérez, and Cordelia Schmid, "Aggregating local image descriptors into compact codes," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 34, no. 9, pp. 1704–1716, 2012.

[3] F. Perronnin and C. Dance, "Fisher kernels on visual vocabularies for image categorization," in *Proceedings of the IEEE International Conference on Computer Vision and Pattern Recognition*, 2007.

[4] Ahmet Iscen, Teddy Furon, Vincent Gripon, Michael Rabbat, and Hervé Jégou, "Memory vectors for similarity search in high-dimensional spaces," *IEEE Transactions on Big Data*, 2017.

[5] Marzieh Gheisari, Teddy Furon, Laurent Amsaleg, Behrooz Razeghi, and Slava Voloshynovskiy, "Aggregation and embedding for group membership verification," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing*, 2019.

[6] Marzieh Gheisari, Teddy Furon, and Laurent Amsaleg, "Privacy preserving group membership verification and identification," in *Proceedings of the The IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, June 2019.

[7] Marzieh Gheisari, Teddy Furon, and Laurent Amsaleg, "Group membership verification with privacy: Sparse or dense?," in *Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS)*, 2019.

[8] Behrooz Razeghi, Slava Voloshynovskiy, Dimche Kostadinov, and Olga Taran, "Privacy preserving identification using sparse approximation with ambiguization," in *Proceedings of the IEEE International Workshop on Information Forensics and Security*, 2017.

[9] Behrooz Razeghi and Slava Voloshynovskiy, "Privacy-preserving outsourced media search using secure sparse ternary codes," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing*, 2018.

[10] Peter H. Schönemann, "A generalized solution of the orthogonal procrustes problem," *Psychometrika*, vol. 31, no. 1, pp. 1–10, 1966.

[11] Omkar M Parkhi, Andrea Vedaldi, Andrew Zisserman, et al., "Deep face recognition.," in *Proceedings of the British Machine Vision Conference*, 2015.

[12] Gary B Huang, Marwan Mattar, Tamara Berg, and Eric Learned-Miller, "Labeled faces in the wild: A database forstudying face recognition in unconstrained environments," in *Workshop on faces in'Real-Life'Images: detection, alignment, and recognition*, 2008.

[13] Soumyadip Sengupta, Jun-Cheng Chen, Carlos Castillo, Vishal M Patel, Rama Chellappa, and David W Jacobs, "Frontal to profile face verification in the wild," in *Proceeding of the IEEE Winter Conference on Applications of Computer Vision*, 2016.

[14] Chinese Academy of Sciences Institute of Automation, "Casia-irisv1 iris image database [online]," *Available: http://www.cbsr.ia.ac.cn/IrisDatabase.htm*.

[15] The Multimedia University, "Mmu2 iris image database [online]," *Available: http://pesona.mmu.edu.my/ ccteo/*.

[16] Pascal Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Advances in Cryptology — EUROCRYPT '99*, Jacques Stern, Ed., Berlin, Heidelberg, 1999, pp. 223–238, Springer Berlin Heidelberg.

[17] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, July 1985.